Amendments to the Specification

Please replace the paragraph on Page 1, lines 5 - 8 with the following marked-up replacement paragraph:

-- The present invention is related to U. S. Patent _____ (serial ~~number 09/_____~~), ~~titled~~ number 09/614,087), titled "Technique for Synchronizing Security Credentials using a Trusted Authenticating Domain", which is commonly assigned to the International Business Machines Corporation (IBM) and which was filed concurrently herewith on [[__/__/]] July 11, 2000. --

Please replace the paragraph on Page 14, lines 5 - 6 with the following marked-up replacement paragraph:

-- Figure 4 depicts a flow chart which sets forth a preferred embodiment of the logic involved in implementing the scenario illustrated in Figure [[4]] 3; --

Please replace the paragraph that begins on Page 23, line 28 and carries over to Page 24, line 12 with the following marked-up replacement paragraph:

-- The logic with which this process operates is depicted in more detail in Fig. 4. At 401, the user initiates the synchronization process by connecting to the synchronization agent. The agent then prompts the user (402) to enter his/her security credentials. The user provides those credentials (403), and the agent then performs the validation by communicating with the master registry (404). A test is made to determine whether the validation was successful (405); if not, an error is preferably reported to the user (409). The user may be given another chance to re-enter

the credentials, if desired (not shown in Fig. 4); preferably, a relatively low upper limit is imposed on the number of times the user is allowed to retry the operation, in order to prevent security exposures such as brute force attacks. When the validation was successful, the password synchronization policy is interrogated (406) to see if this user's credentials are to be propagated to one or more other registries. If so, then the credentials which the user entered at [[402]] 403 are forwarded to those target registries (408). A message is preferably provided to the user (409) indicating that the propagation has occurred, or that there were no propagation targets registered. The processing of Fig. 4 then ends. --

Please replace the paragraph that begins on Page 25, line 3 and carries over to Page 26, line 11 with the following marked-up replacement paragraph:

-- As shown in Fig. 5, the user connects 501 to the password synchronization agent [[520]] 510 using a web browser, telnet client, or other similar client program 500. As in the first preferred embodiment described above, this connection between the user client and the password synchronization agent should be encrypted and the password synchronization agent should be authenticated to the client, using SSL or similar means. The user's ID and password (or other secret identifying information) are sent to the password synchronization agent over this secure connection. The user may also explicitly specify the authenticating domain (meaning a trusted target registry [[540]] 530 to be used in authenticating the user) as part of this transmission, or trust policies within the master registry [[530]] 520 may identify that trusted registry [[540]] 530. The password synchronization agent then connects to the master registry to look up the trust and password synchronization policies (502, 503). As described for the first preferred embodiment,

these may be specified on a per-user basis, or for the entire master registry, or for subsets of the entries in the master registry. The password synchronization agent looks in the master registry for a trust policy that applies to the current user. If: (a) such a policy is found, and (b) it indicates that the authenticating domain indicated by the user is a trusted registry for that user's entry in the master registry, or (c) the user did not specify the authentication domain but the policy does, then the password synchronization agent authenticates the user with the trusted registry (504, 505). If this authentication succeeds, the password synchronization agent updates 506 the user's password (or other secret security credential) in the master registry. It then reports 507 the results to the user. The user's password or security credential may then be updated in other target registries, either by the password synchronization agent itself or by the update process of a meta-directory connector of the type which has been previously described (508, 509). In the preferred embodiment, the password synchronization agent must be configured with an administrative identity and corresponding authentication credential for the master registry, and if the password synchronization agent itself performs password updates for target registries, it must be configured with an administrative identity and corresponding authentication credential for these as well. All connections between the password synchronization agent and the master, trusted, and target registries should be protected by encryption and by an authentication process for each target server, via SSL or similar means. --